Ethical Hacking and Countermeasures

Version 11

Lab Manual

EC-Council

Copyright © 2020 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

9h]W' < UW]b[UbX7ci bHYfa YUg fYg Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	-
02	Footprinting and Reconnaissance	01
03	Scanning Networks	180
04	Enumeration	317
05	Vulnerability Analysis	410
06	System Hacking	494
07	Malware Threats	710
08	Sniffing	881
09	Social Engineering	1027
10	Denial-of-Service	1084
11	Session Hijacking	1123
12	Evading IDS, Firewalls, and Honeypots	1150
13	Hacking Web Servers	1215
14	Hacking Web Applications	1262
15	SQL Injection	1424
16	Hacking Wireless Networks	1470
17	Hacking Mobile Platforms	1560
18	IoT and OT Hacking	1618
19	Cloud Computing	1649
20	Cryptography	1679

9h\ ]W'< UW]b[`UbX7ci bHYfa YUgj fYg Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.